1 Билет 14

Основная теорема арифметики в $\mathbb{Z}[t]$

Определение

Многочлен $f \in \mathbb{Z}[t]$ — *тривиальный*, если $c(f) = 1$.

Теорема 4

Любой многочлен $f \in \mathbb{Z}[x]$ с положительным старшим коэффициентом раскладывается в произведение $f = r_1 \dots r_k \cdot p_1 \dots, p_n$, где $r_1, \dots, r_k \in \mathbb{P}$, а $p_1, \dots, p_n \in \mathbb{Z}[x]$ — тривиальные неприводимые многочлены с положительными старшими коэффициентами. Разложение единственно с точностью до перестановки сомножителей.

• Разумеется, многочлен $f \in \mathbb{Z}[x]$ с отрицательным старшим коэффициентом раскладывается в аналогичное произведение $f = -r_1 \dots r_k \cdot p_1 \dots, p_n$.

Доказательство. $\exists$ • Пусть $f = c(f) \cdot g$, тогда $g \in \mathbb{Z}[x]$ и $c(g) = 1$. По ОТА в $\mathbb{Z}$ существует разложение на простые множители $c(f) = r_1 \dots r_k$.

• Пусть a — старший коэффициент g. Тогда $a > 0$.

• По ОТА в $\mathbb{Q}[x]$ существует разложение $g = aq'_1 q_2 \dots q_n$, где $q'_1, q_2, \dots, q_n$ — неприводимые в $\mathbb{Q}[x]$ многочлены.

• Положим $q_1 := aq'_1$, тогда q_1 также неприводим в $\mathbb{Q}[x]$.

• Итак, $g = q_1 q_2 \dots q_n$.

• По Лемме 9 существует разложение $g = p_1 \dots p_n$, где $p_i \in \mathbb{Z}[x]$ и $p_i = c_i q_i$, $c_i \in \mathbb{Q}$.

• Можно считать, что старший коэффициент каждого p_i положителен: иначе заменим p_i на $-p_i$ и c_i на $-c_i$.

• Так как $p_i \sim q_i$ в $\mathbb{Q}[x]$, многочлены $p_1, \dots, p_n$ неприводимы в $\mathbb{Q}[x]$, а значит, и в $\mathbb{Z}[x]$.

• Тогда $f = r_1 \dots r_k \cdot p_1 \dots p_n$.

• По Следствию 1 имеем $c(f) = c(r_1 \dots r_k \cdot p_1 \dots p_n) = r_1 \dots r_k \cdot c(p_1) \dots c(p_n) = c(f) \cdot c(p_1) \dots c(p_n)$, откуда $c(p_1) = \dots c(p_n) = 1$.

• Значит, $f = r_1 \dots r_k \cdot p_1 \dots p_n$.— искомое разложение.

! • Предположим, что разложение не единственно:

$$f = r_1 \dots r_k p_1 \dots p_n = s_1 \dots s_\ell q_1 \dots q_m, \qquad (1)$$

где $r_1, \dots, r_k, s_1, \dots, s_\ell \in \mathbb{P}$ и $p_1 \dots p_n, q_1 \dots q_m \in \mathbb{Z}[x]$ — неприводимые тривиальные многочлены с положительными старшими коэффициентами.

• По Лемме 8, тогда $c(p_1 \dots p_n) = c(p_1) \dots c(p_n) = 1$, откуда $c(f) = r_1 \dots r_k$ — разложение на простые множители. Аналогично, $c(f) = s_1 \dots s_\ell$ — разложение на простые множители.

• По ОТА в $\mathbb{Z}$, эти разложения могут отличаться только порядком множителей, что нам и надо.

• Пусть $g := \frac{1}{c(f)} f \in \mathbb{Z}[x]$, тогда $g = p_1 \dots p_n = q_1 \dots q_m$ — два разложения g в произведение неприводимых в $\mathbb{Z}[x]$ тривиальных многочленов.

• По Следствию 2 это два разложения g в произведение неприводимых многочленов в $\mathbb{Q}[x]$.

- Пусть p_i^* — многочлен, полученный из p_i делением на старший коэффициент (для всех $i \in \{1, \ldots, n\}$), а q_j^* — многочлен, полученный из q_j делением на старший коэффициент (для всех $j \in \{1, \ldots, m\}$), а a — старший коэффициент f.
- Тогда $g = ap_1^* \ldots p_n^* = aq_1^* \ldots q_m^*$ — два разложения g в $\mathbb{Q}[x]$ в произведение неприводимых многочленов со старшим коэффициентом 1, а по ОТА в $\mathbb{Q}[x]$ (Теорема 3.5) такие разложения могут отличаться лишь порядком сомножителей.
- Значит, $m = n$ и можно считать, что $p_i^* = q_i^*$ для всех i.
- Тогда существует такое $c_i \in \mathbb{Q}$, что $p_i = c_i q_i$. Тогда $c_i > 0$ (так как c_i равно отношению положительных старших коэффициентов p_i и q_i).
- Нам остается доказать, что $c_1 = \cdots = c_n = 1$. Пусть это не так. Из (1) ясно, что $c_1 c_2 \ldots c_n = 1$. Значит, НУО $c_1 > 1$.
- Пусть $c_1 = \frac{a_1}{b_1}$ — представление в виде несократимой дроби. Тогда $(a_1, b_1) = 1$, $a_1 > 1$.
- Пусть $q_1(t) = d_w t^w + \cdots + d_0$, тогда $p_1(t) = \frac{a_1 d_w}{b_1} t^w + \cdots + \frac{a_1 d_0}{b_1}$.
- Так как $(a_1, b_1) = 1$, для всех $i \in \{1, \ldots, w\}$ мы имеем $\frac{a_1 d_i}{b_1} \vdots a_1$. Значит, $1 = c(p_1) \vdots a_1$, противоречие.

Альтернативно одарённое доказательство:
f - многочлен в Z[x]
Переведём его в Q[x], где он имеет единственное разложение на неприводимые .
$f_q = a \cdot q_1 q_2 \cdot \ldots \cdot q_n$
Тогда по Лемме 9:
$\forall q_i \exists p_i \in Z, c_i \in Q : p_i = c_i \cdot q_i$
Т.к p$\sim q$, то p неприводим в $Q[x] \rightarrow$ неприводим и в Z[x].
Тогда $f = r_1 r_2 ... r_k p_1 p_2 ... p_n$ - искомое разложение
Единственность разложения в Z[x], на мой взгляд, следует из единственности в Q[x]

2 Билет 14

Критерий Эйзенштейна

Теорема 5

Пусть $f(x) = a_n t^n + \dots + a_1 t + a_0 \in \mathbb{Z}[t]$ *и* $p \in \mathbb{P}$ *таковы, что* $a_n \not\vdots\, p$, $a_{n-1}, \dots, a_0 \,\vdots\, p$ *и* $a_0 \not\vdots\, p^2$. *Тогда* f *— неприводим в* $\mathbb{Z}[t]$.

Доказательство. • Предположим противное. Пусть $f = gh$, где $\deg(g) > 0$ и $\deg(h) > 0$.

• Пусть $g(t) = b_m t^m + \dots + b_0$, $h(t) = c_k t^k + \dots + c_0$ (тогда $m + k = n$).

• Так как $c_0 b_0 = a_0 \,\vdots\, p$ и $c_0 b_0 \not\vdots\, p^2$, НУО $b_0 \,\vdots\, p$ и $c_0 \not\vdots\, p$.

• Так как $b_m c_k = a_n \not\vdots\, p$, мы имеем $b_m \not\vdots\, p$. Следовательно, можно выбрать наименьший такой индекс ℓ, что $b_\ell \not\vdots\, p$.

• Тогда $a_\ell = b_\ell c_0 + \sum\limits_{i=0}^{\ell-1} b_i c_{\ell-i} \not\vdots\, p$, так как $b_\ell c_0 \not\vdots\, p$, а для всех $i \in \{0, \dots, \ell - 1\}$ $b_i \,\vdots\, p$.

• Значит, $a_\ell \not\vdots\, p$. Но $\ell \le m < n$, противоречие. □

Следствие 3

Пусть $f(x) = a_n t^n + \dots + a_1 t + a_0 \in \mathbb{Z}[t]$ *и* $p \in \mathbb{P}$ *таковы, что* $a_0 \not\vdots\, p$, $a_1, \dots, a_n \,\vdots\, p$ *и* $a_n \not\vdots\, p^2$. *Тогда* f *— неприводим в* $\mathbb{Z}[t]$.

• Доказательство аналогично Теореме 5.